AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Claims 1-43. (Cancelled)

44. (new) A tamper-resistant security device having means for storing user credentials, including at least a security key, an Authentication and Key Agreement (AKA) module for performing an AKA process with said security key, and means for external communication,

wherein said tamper-resistant security device further comprises:

- an application for cooperation with said AKA module; and
- means for interfacing said AKA module and said cooperating application.

45. (new) The tamper-resistant security device according to claim 44, wherein said cooperating application performs enhanced security processing of at least one parameter associated with said AKA process.

46. (new) The tamper-resistant security device according to claim 45, wherein said enhanced security processing includes at least one of:

- pre-processing of at least one AKA input parameter; and
- post-processing of at least one AKA output parameter.

47. (new) The tamper-resistant security device according to claim 45, wherein said enhanced security processing includes encapsulation of said at least one AKA parameter.

48. (new) The tamper-resistant security device according to claim 45, wherein said cooperating application is receiving at least one AKA parameter from said AKA process to generate a further AKA parameter that has higher security than said received AKA parameter.

49. (new) The tamper-resistant security device according to claim 45, wherein said enhanced security processing includes evaluation of a predetermined number of consecutive AKA input parameters for verifying that said AKA input parameters can be used securely.

50. (new) The tamper-resistant security device according to claim 49, wherein said enhanced security processing further includes combination of a predetermined number of consecutive AKA output parameters generated in response to a number of corresponding unique AKA input parameters.

51. (new) The tamper-resistant security device according to claim 44, further comprising means for performing security policy processing based on information representative of security conditions in relation to said tamper-resistant security device.

52. (new) The tamper-resistant security device according to claim 51, wherein the security conditions reflect at least one of the environment in which said security device is operated and the network interface over which a request for AKA processing originates.

53. (new) The tamper-resistant security device according to claim 51, wherein said security policy processing includes at least one of a security policy decision process and a security policy enforcement process.

54. (new) The tamper-resistant security device according to claim 51, wherein said means for performing security policy processing comprises means for selectively disabling direct access to said AKA module.

55. (new) The tamper-resistant security device according to claim 51, wherein said tamper-resistant security device comprises means for detecting whether said tamper-resistant security device is operated in its normal environment or in an environment considered insecure, and said means for performing security policy processing comprises means for disabling direct access to said AKA module when operated in said insecure environment.

56. (new) The tamper-resistant security device according to claim 44, wherein

said cooperating application includes a security enhancing application, and said security device further comprises means for transferring a request for AKA processing directly to said AKA module if said security device is operated in an environment considered secure, and means for transferring said request to said security enhancing application if said security device is operated in an environment considered insecure.

57. (new) The tamper-resistant security device according to claim 44, wherein said cooperating application is performing at least part of the computations in connection with end-to-end key agreement between users.

58. (new) The tamper-resistant security device according to claim 44, wherein said cooperating application is masking key information generated by said AKA module.

59. (new) The tamper-resistant security device according to claim 44, wherein said cooperating application is a software application installed in an application environment of said tamper-resistant security device.

60. (new) The tamper-resistant security device according to claim 59, wherein said application is securely downloaded into said tamper-resistant security device from a trusted party.

61. (new) The tamper-resistant security device according to claim 44, wherein

said cooperating application is a privacy enhancing application, which participates in managing a user pseudonym.

62. (new) The tamper-resistant security device according to claim 61, wherein said privacy enhancing application is requesting an AKA response from said AKA module based on an old user pseudonym and for generating a new user pseudonym based on the received AKA response.

63. (new) A tamper-resistant security device having means for storing user credentials, including at least a security key, an Authentication and Key Agreement (AKA) module for performing an AKA process with said security key, and means for external communication,

wherein said tamper-resistant security device further comprises a software application implemented in an application environment of said tamper-resistant security device and adapted for cooperating with said AKA module, and said AKA module is also implemented, at least partly, as a software application in said application environment.

64. (new) A user terminal provided with a tamper-resistant security device, said tamper-resistant security device having means for storing user credentials, including at least a security key, an Authentication and Key Agreement (AKA) module for performing an AKA process with said security key, and means for communication with said user terminal,

wherein said tamper-resistant security device further comprises:

- an application for cooperation with said AKA module; and
- means for interfacing said AKA module and said cooperating application.

65. (new) The user terminal according to claim 64, wherein said cooperating application is at least one of a security enhancing application and a privacy enhancing application.

66. (new) The user terminal according to claim 64, wherein said cooperating application is performing enhanced security processing of at least one parameter associated with said AKA process.

67. (new) The user terminal according to claim 66, wherein said enhanced security processing includes encapsulation of said at least one AKA parameter for producing an output parameter of higher security than said at least one AKA parameter.

68. (new) The user terminal according to claim 64, further comprising means for performing security policy processing based on information representative of security conditions in relation to said tamper-resistant security device.

69. (new) The user terminal according to claim 68, wherein the security conditions reflect at least one of the environment in which said security device is

operated, the network interface over which a request for AKA processing comes, and the network used by the user terminal for network communication.

70. (new) The user terminal according to claim 68, wherein said security policy processing includes at least one of a security policy decision process and a security policy enforcement process.

71. (new) The user terminal according to claim 68, wherein said means for performing security policy processing is implemented in said tamper-resistant security device for selectively disabling direct access to said AKA module.

72. (new) The user terminal according to claim 64, wherein said cooperating application is a security enhancing application, and said security device further comprises means for transferring a request for AKA processing directly to said AKA module if said security device is operated in an environment considered secure, and means for transferring said request to said security enhancing application if said security device is operated in an environment considered insecure.

73. (new) The user terminal according to claim 64, wherein said cooperating application includes a security enhancing application, and said user terminal further comprises means for transferring a request for AKA processing directly to said AKA module if said request comes over an interface considered secure, and means for

transferring said request to said security enhancing application if said request comes over an interface considered insecure.

74. (new) The user terminal according to claim 73, wherein said security enhancing application comprises a number of different security enhancing modules, and said security enhancing application is for selecting among said security enhancing modules in dependence on the type of interface.

75. (new) · The user terminal according to claim 64, wherein said cooperating application is a software application installed in an application environment of said tamper-resistant security device.

76. (new) The user terminal according to claim 64, wherein said cooperating application includes a security enhancing application authenticating a network over which said user terminal intends to communicate.

77. (new) A network server managed by a trusted party sharing a security key with a tamper-resistant security device implemented in a user terminal, said tamper-resistant security device having an Authentication and Key Agreement (AKA) module for performing an AKA process with said security key,

wherein said network server comprises means for downloading a software application adapted for interfacing and cooperating with said AKA module into an application environment of said tamper-resistant device.

78. (new) The network server according to claim 77, wherein said download application is at least one of a security enhancing application, a privacy enhancing application, and a security policy application.